



PATENT OFFICE  
JAPANESE GOVERNMENT

RECEIVED

NOV 15 1999

Group 2700

This is to certify that the annexed is a true copy  
of the following application as filed with this office.

Date of Application: September 4, 1998

Application Number: Japanese Patent Application  
No. 10-251193

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE  
CORPORATION

August 30, 1999

Commissioner,  
Patent Office

Takeshi Isayama (Seal)

. Certificate No.11-3060041



日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

RECEIVED  
NOV 15 1999  
Group 2700

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1998年 9月 4日

出願番号

Application Number:

平成10年特許願第251193号

出願人

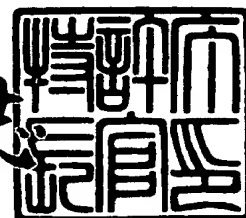
Applicant (s):

日本電信電話株式会社

1999年 8月30日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建志



出証番号 出証特平11-3060041

【書類名】 特許願

【整理番号】 NTTH105937

【提出日】 平成10年 9月 4日

【あて先】 特許庁長官殿

【国際特許分類】 G06C

【発明の名称】 抽出電子透かし情報統計処理方法、その装置及びプログラム記憶媒体

【請求項の数】 16

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19 番 2 号 日本電信電話株式会社内

    【氏名】 小川 宏

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19 番 2 号 日本電信電話株式会社内

    【氏名】 中村 高雄

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19 番 2 号 日本電信電話株式会社内

    【氏名】 富岡 淳樹

【発明者】

    【住所又は居所】 東京都新宿区西新宿三丁目 19 番 2 号 日本電信電話株式会社内

    【氏名】 高嶋 洋一

【特許出願人】

    【識別番号】 000004226

    【氏名又は名称】 日本電信電話株式会社

【代理人】

    【識別番号】 100066153

【弁理士】

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【弁理士】

【氏名又は名称】 稲垣 稔

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 抽出電子透かし情報統計処理方法、その装置及びプログラム記憶媒体

【特許請求の範囲】

【請求項1】 情報コンテンツに埋め込まれた電子透かし情報を再構成する方法において、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて、情報コンテンツに埋め込まれていた電子透かし情報を再構成することを特徴とする抽出電子透かし情報統計処理方法。

【請求項2】 請求項1記載の方法において、

抽出した電子透かし情報の信頼度のしきい値を予め決めておき、

情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率を、情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率から得られる二項分布に基づいて計算し、

その出現確率又は $1 - \text{出現確率}$ が上記信頼度のしきい値を超えている場合のみ電子透かし情報を再構成し、超えていない場合は電子透かし無しもしくは不明と判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項3】 請求項2記載の方法において、

抽出した電子透かし情報を再構成するのに、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率から判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項4】 請求項1乃至3の何れかに記載の方法において、

電子透かし情報とその信頼性を、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の、情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求めることを特徴とする抽出電子透かし情報統計処理方法。

【請求項5】 請求項1乃至4の何れかに記載の方法において、

電子透かし情報として実際に埋め込まれる情報系列を疑似乱数系列により予め

変調しておき、

電子透かし情報再構成処理の前に電子透かし埋め込みに用いた同じ疑似乱数系列で復調することを特徴とする抽出電子透かし情報統計処理方法。

【請求項6】 請求項5記載の方法において、

情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率を共に $1/2$ に固定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項7】 情報コンテンツに埋め込まれた電子透かし情報を再構成する装置であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する抽出手段を有することを特徴とする抽出電子透かし情報統計処理装置。

【請求項8】 請求項7記載の装置において、

上記抽出手段は、情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率と電子透かし情報長から二項分布を求める手段と、

上記情報コンテンツの各ビット値に関して電子透かし系列を抽出する手段と、

上記抽出した電子透かし情報の出現確率を、上記求めた二項分布から求める手段と、

その求めた出現確率が信頼度のしきい値より大きいかな否かを判定する手段と、

上記しきい値より大きいと判定された情報について電子透かし情報を再構成する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項9】 請求項8記載の装置において、

上記求めた出現確率から、上記再構成した情報ビットについての信頼度を求めて、その再構成情報ビットと共に出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項10】 請求項7乃至9の何れかに記載の装置において、

電子透かし情報として実際に埋め込まれる情報系列を疑似乱数系列により予め変調する手段と、

電子透かし情報再構成処理の前に電子透かし埋め込みに用いた同じ疑似乱数系

列で復調する手段を有することを特徴とする抽出電子透かし情報統計処理装置。

【請求項 11】 情報コンテンツに埋め込まれた電子透かし情報を再構成するプログラムを格納した記憶媒体であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する処理を

コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項 12】 請求項 11 記載の記憶媒体において、

抽出した電子透かし情報の信頼度のしきい値を予め決めておき、

情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率を、

情報コンテンツから任意に抽出した 1 ビット系列の各ビットの出現確率から得られる二項分布に基づいて計算する処理と、

その計算した出現確率又は  $1 - \text{出現確率}$  が信頼度のしきい値を超えている場合のみ電子透かし情報を再構成し、超えていない場合は電子透かし無しもしくは不明と判定する処理とを上記プログラムが有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項 13】 請求項 12 記載の記憶媒体において、

抽出した電子透かし情報を再構成するのに、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率から判定する処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項 14】 請求項 11 乃至 13 の何れかに記載の記憶媒体において、

電子透かし情報とその信頼性を、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の、情報コンテンツから任意に抽出した 1 ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求める処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項 15】 請求項 11 乃至 14 の何れかに記載の記憶媒体において、

電子透かし情報として実際に埋め込まれる情報系列を疑似乱数系列により予め

変調しておき、電子透かし情報再構成処理の前に電子透かし埋め込みに用いた同じ疑似乱数系列で復調する処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項 16】 請求項 15 の記憶媒体において、

情報コンテンツから任意に抽出した 1 ビット系列の各ビットの出現確率を共に  $1/2$  に固定する処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

マルチメディア著作物は、不正複製や改竄（かいざん）が容易であることから、情報利用者の正当な二次利用やコンテンツ提供者の情報発信の障害となっており、その著作権保護が訴えられている。画像や音声などのメディアの冗長性を利用し、人間に知覚されないように主情報である情報コンテンツに別の副情報を埋め込む技術に『電子透かし技術』がある。この技術は、重畳した情報の分離が困難なことより、マルチメディア著作物の著作権保護に有効な手段として考えられている。この発明は、電子透かしを用いたシステムにおける、抽出透かし情報の統計処理に関する方法及びその装置及び抽出情報の統計処理プログラムを格納した記憶媒体に関するものである。

【0002】

【従来技術】

特願平 8-305370 もしくは特願平 8-338769 もしくは特願平 9-9812 もしくは特願平 9-14388 もしくは特願平 9-57516 もしくは特願平 9-109924 もしくは特願平 9-164466 もしくは特願平 9-197003 もしくは特願平 9-218467 もしくは特願平 10-33239 などに記載の電子透かし技術（Digital Watermark, Data Hiding, Finger Printing, Steganography, 画像・音声深層暗号などとも呼ぶ）を用いたシステムにおいて一番重要な問題は、埋め込んだ情報の有無の判定および埋め込んだ情報の信頼性の精度であ



る。電子透かしシステムは、電子透かしを埋め込んだ情報コンテンツに対する様々なメディア処理を想定して、情報コンテンツに埋め込まれている副情報（以下電子透かし情報と呼ぶことにする）がある程度壊れていても、正しい電子透かし情報を再構成する機構を持っているものが一般的である。しかしながら現状は、再構成した透かし情報の正当性を定量評価できないものがほとんどであり、信頼性に欠けるものであった。

#### 【0003】

##### 【発明が解決しようとする課題】

電子透かし情報を読みとった際に起こる問題である、電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価できる方法を、装置、プログラム記憶媒体を提供することをこの発明は目的とする。

#### 【0004】

##### 【課題を解決するための手段】

電子透かし処理は、電子透かし埋め込み・電子透かし抽出の対から成る。電子透かし埋め込み処理では、秘密鍵情報などを用いて、情報コンテンツ内の電子透かし対象領域Aから電子透かし埋め込み領域 $B \subseteq A$ を選定し、固有の規則で領域B内のデータを変更する。電子透かし抽出処理では、電子透かし埋め込み領域Bのデータを解釈し、電子透かし情報を再構成する。この発明では、電子透かしが埋め込まれている情報コンテンツにおいて、この発明適用対象となる電子透かしアルゴリズムを用いて、電子透かし対象領域の全体であるAから正誤を問わず任意の秘密鍵情報を用いて読みとられる電子透かし情報の統計学における二項分布をもとに、正しい秘密鍵情報を用いて透かし埋め込み領域Bから読みとられた電子透かし情報がどの程度確率的に起こり得るのかを判定する。

#### 作用

この発明によれば、電子透かし技術において、情報コンテンツから読みとった透かし情報の信頼性を定量的に評価でき、電子透かしが入っていない情報コンテンツを有りと判断したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを読みとったりする確率を一定の値で抑えることができる。

【0005】

【発明の実施の形態】

実施例1

予め意味が曖昧な言葉の定義を行なっておく。

電子透かし系列とは、情報コンテンツから読み出された再構成処理を行なう以前の情報系列を表し、電子透かし情報とは、情報コンテンツに本当に重畳したい、システムの運用上意味ある情報、もしくは、電子透かし系列を再構成処理し得られる情報を表すものとする。

【0006】

同様に埋め込み系列とは、実際に埋め込まれる情報を表し、埋め込み情報を変調したり、引き伸ばしたり、繰り返したりしている系列になっている。

以下にこの発明の実施例1を図面を参照して説明する。

図1は、この発明の背景となる電子透かしシステムの概要図である。

電子透かし情報101は、電子透かし埋め込み装置102によって情報コンテンツ103に埋め込まれ、電子透かし入り情報コンテンツ104に変換される。

【0007】

電子透かし入り情報コンテンツ104は、無線・有線・パッケージ媒体などで流通する間に、情報圧縮やメディア処理などによって品質劣化した電子透かし入り情報コンテンツ105に変化する。

この発明の要部である電子透かし情報再構成装置106は電子透かし抽出装置107内部に実装され、電子透かし抽出装置107を用いて、劣化した電子透かし入り情報コンテンツ105から読みとった電子透かし系列を電子透かし情報再構成装置106を用いて処理し、抽出電子透かし情報108を抽出するという構成になる。

【0008】

以上が電子透かし埋め込み・抽出手順の概要である。

以下、電子透かし情報再構成処理の動作を詳細に説明する。

図2は、電子透かし抽出装置107の内部に実装された電子透かし情報再構成装置106の概要である。

電子透かし情報再構成装置 106 は、電子透かし抽出装置 107 を利用して、電子透かし情報の全埋め込み対象領域から任意の 1 ビット電子透かし系列を抽出したときにビット 1 が抽出される確率  $q$  を予め求めておく。

【0009】

すなわち、1 ビット電子透かし系列抽出処理部 201 のようなものを仮定し、電子透かし対象領域の全要素に対して 1 ビットずつ電子透かし系列の抽出を行ない（破線 L1）、この全試行のうちビット 1 が何回取り出されたかの率を計算する。

この実施例ではビット 1 の抽出確率および個数を求めているが、ビット 0 の抽出確率および個数を求めても実装上の違いのみであり、本質的に変わらないことを留意しておく。

【0010】

これより、電子透かしアルゴリズムを用いて、情報コンテンツ 105 の電子透かし対象領域から無作為に 1 ビット電子透かし系列の抽出を行なったときのビット 0 と 1 の出現確率はそれぞれ  $1 - q$  および  $q$  と計算される。

$n$  ビット電子透かし系列抽出処理装置 202 は、電子透かしが埋め込まれている情報コンテンツから電子透かしが埋め込まれたのべ回数だけ電子透かし系列の抽出を行なう。

【0011】

ここで、電子透かし情報を  $b_0 \ b_1 \ \dots \ b_{m-1}$ 、 $b_i \in \{0, 1\}$ 、 $i < m$ （情報長  $m$  ビット）、 $i$  ビット目の電子透かし情報を情報コンテンツに埋め込んだ繰り返し回数（拡散率、chip-rate などとも呼ぶ）を  $n_i$  回、読みとった電子透かし系列を

$$\begin{aligned} & b'_{0,0} \ b'_{0,1} \ \dots \ b'_{0,n_0-1} \ b'_{1,0} \ b'_{1,1} \ \dots \ b'_{1,n_1-1} \ \dots \\ & \quad b'_{m-1,0} \ b'_{m-1,1} \ \dots \ b'_{m-1,n_{m-1}-1} \\ & \quad b'_{i,j} \in \{0, 1\} \end{aligned}$$

（長さ  $\sum_{r=0}^{m-1} n_r$  ビット列）と定義する。

【0012】

電子透かし情報再構成装置 106 は、 $n$  ビット電子透かし情報抽出処理部 20

2から、電子透かし情報の0番目に相当する電子透かし系列の部分列から $m-1$ 番目に相当する電子透かし系列の部分列までを順次入力として受けとる（実線L2）。

次に、実際に電子透かし情報の $i$ ビット目の電子透かし情報を再構成する方法を具体的に述べる。

【0013】

電子透かし対象領域から任意に $n_i$ ビット電子透かし系列の抽出を行なったとき、この $n_i$ ビット列にビット1が $k$ 個現れる確率 $P(x=k)$ は、二項分布の密度関数によって

$$P(x=k) = n_i C_k q^k \cdot (1-q)^{n_i-k} \quad (1)$$

で表され、その分布関数 $F(x)$ は、

$$F(x) = \sum_{k=0}^x n_i C_k q^k \cdot (1-q)^{n_i-k} \quad (2)$$

$$(0 \leq x \leq n_i)$$

である。ただし、 $n_i C_k$ は、 $n_i$ 個の中から $k$ 個のものを選ぶ組合せ数を表す。

【0014】

電子透かし情報の信頼度のしきい値 $\alpha$  ( $1/2 < \alpha \leq 1$ ) を設け、電子透かし情報再構成装置106に入力された電子透かし情報の $i$ 番目に相当する電子透かし系列の部分列 $b'_{i,0} b'_{i,1} \dots b'_{i,n_i-1}$ に含まれるビット1の数を

$$k_i = \sum_{r=0}^{n_i-1} b'_{i,r}$$

によって計算し、式(2)を用いて電子透かし情報を

$$b_i = \begin{cases} 0 & 0 \leq F(k_i) \leq 1-\alpha \text{ のとき} \\ 1 & \alpha \leq F(k_i) \leq 1 \text{ のとき} \\ \text{不明もしくは無し} & 1-\alpha < F(k_i) < \alpha \text{ のとき} \end{cases} \quad (3)$$

と判定する。

【0015】

見方を変えて電子透かし系列 $n_i$ に含まれるビット1の個数によって判定すると、 $0 \leq F(x=x_0) \leq 1-\alpha$ を満たす最大の $x_0$ と、 $\alpha \leq F(x=x_1) \leq 1$ を満たす最小の $x_1$ をしきい値として、図3に示すように $n_i$ 個中の1が $x_0$

以下なら0と、 $x_1$  以上なら1と透かし情報を判定する。

図3の横軸は電子透かし系列に含まれるビット1の個数、縦軸はその出現頻度を表す。

【0016】

電子透かしシステムによっては、情報コンテンツ105から抽出された電子透かし系列の分布 $P(x)$ の中心値に対する偏りから再構成した電子透かし情報を求め、抽出された電子透かし系列が統計的にどの程度の確率で出現するのかを式(2)の値で求めて、再構成された電子透かし情報が1の場合は $F(k_i)$ を、情報が0の場合は $1 - F(k_i)$ を電子透かしの信頼度として付加して出力することも可能である。この電子透かしの信頼度 $F(k_i)$ 、 $1 - F(k_i)$ は、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の、情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求めたものになる。

【0017】

この処理を電子透かし情報の情報長 $m$ ビットに拡張した概念を図4に示す。

電子透かし情報再構成装置106は、再構成した電子透かし情報 $b_0 b_1 \dots b_{m-1}$ を抽出電子透かし情報108として出力する。

以上が電子透かし情報再構成処理の動作についてである。

この処理の手順を図5に示す。電子透かし入り情報コンテンツ105と、電子透かし情報抽出に必要な秘密情報が入力され、その情報コンテンツ105から任意に抽出した1ビット系列の各ビットの出現確率と電子透かし情報長から二項分布 $F(x)$ を予め求める、つまり式(2)を求める(S1)。一方情報コンテンツ105と秘密情報とを用いて、各ビット値に関して、電子透かし系列を抽出する(S2)。その抽出した電子透かし情報 $k_i$ の出現確率 $F(k_i)$ を、予め求めておいた二項分布 $F(x)$ から求める(S3)。この出現確率 $F(k_i)$ に対し判定式(3)を適用する。換言すると、 $F(k_i)$ 、又は $1 - F(k_i)$ が信頼度のしきい値 $\alpha$ より大きいか否かの判定を行い(S4)、しきい値 $\alpha$ より大であれば、電子透かし情報を再構成する(S5)。つまり $F(k_i) > \alpha$ であれば

、その電子透かし情報を 1 とし、 $1 - F(k_i) > \alpha$  であれば電子透かし情報を 0 とする。このようにしてすべてのビット値に関して再構成処理を終了すると電子透かし情報を出力する。つまりステップ S2 ～ S5 を電子透かしのビット長さだけ繰り返す。ステップ S4 で  $F(k_i)$ 、 $1 - F(k_i)$  の何れもしきい値  $\alpha$  より大でなければ、電子透かし情報は無い、又は電子透かし情報は不明と判定して処理を終了する (S6)。

【0018】

実施例 1 では、式 (1) に表される分布に偏りが無い、つまり、 $q \simeq 1/2$  となることを前提としている。

電子透かし情報のそれぞれのビット埋め込み回数  $n_i$  が、統計的特徴を得るのに十分な数である場合、一般的には、 $q \simeq 1/2$  となるが、 $q$  の値は、電子透かしアルゴリズムと情報コンテンツの特徴に依存するため、稀に  $q$  が  $1/2$  から大きく外れた数となることがある。

【0019】

この問題を回避する方法を実施例 2 で示す。

## 実施例 2

以下にこの発明の実施例 2 を図面を参照して説明する。

図 6 は、この実施例 2 を付加した電子透かしシステムの概要図である。

電子透かし埋め込み装置 102 が情報コンテンツ 103 に電子透かし情報 101 を埋め込む際に、電子透かし情報の各ビット値を  $n_i$  回繰り返して埋め込む処理において、電子透かし埋め込み装置 102 の内部に実装された疑似乱数系列発生器 (甲) 501 を用いて、埋め込み系列を変調し、これを情報コンテンツ 103 に埋め込む。

【0020】

例えば、埋め込み系列を

$$b_{0,0} b_{0,1} \cdots b_{0,n_0-1} b_{1,0} b_{1,1} \cdots b_{1,n_1-1} \cdots b_{m-1,0} b_{m-1,1} \cdots b_{m-1,n_{m-1}-1}$$

$$b_{i,j} \in \{0, 1\}$$

疑似乱数系列を

$$r_{i,0} r_{i,1} \cdots r_{i,n_i-1}$$

$$r_{i,j} \in \{0, 1\}$$

とおくと、埋め込み系列を疑似乱数系列によって

$$m_{i,0} \ m_{i,1} \ \cdots m_{i,n_i-1}$$

$$m_{i,j} = b_{i,j} \ (+) \ r_{i,j}$$

に変調する。A (+) BはAとBの排他的論理和を表わす。

【0021】

この処理により、電子透かし抽出処理には、電子透かし系列埋め込みに用いたのと同じ疑似乱数系列が必要となる。

例えば、疑似乱数系列としてM系列を用いたとする。

すると、任意のM系列を用いて1ビット電子透かし系列抽出を行なったとき  $q \simeq 1/2$  となり、電子透かしアルゴリズムと情報コンテンツに依存することなくこの発明を適用可能となる。

【0022】

電子透かし抽出では、電子透かし抽出装置107の内部に実装された疑似乱数系列発生器(乙)502を用いて、

$$b'_{i,j} = m_{i,j} \ (+) \ r_{i,j}$$

により復調する。

ここで、疑似乱数発生器(甲)501と疑似乱数発生器(乙)502は、同じ疑似乱数系列を発生するように実装する必要がある。

【0023】

復調処理により得られた電子透かし系列

$$b'_{0,0} \ b'_{0,1} \ \cdots b'_{0,n_0-1} \ b'_{1,0} \ b'_{1,1} \ \cdots b'_{1,n_1-1} \ \cdots$$

$$b'_{m-1,0} \ b'_{m-1,1} \ \cdots b'_{m-1,n_{m-1}-1}$$

$$b'_{i,j} \in \{0, 1\}$$

に対して、実施例1で説明した方法により電子透かし情報を再構成する。

【0024】

読みとった電子透かし系列のビット1の出現確率qは、変調の有無に関わらず二項分布に近似できると考えられるため、この実施例で示した変調処理による密度関数の分布(1)への影響はない。

また、実装において、 $q = 1/2$ と仮定できるため、つまり $q$ を求める処理（引算）を行うことなく、式（1）で $q = 1/2$ として計算することにより、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、高速化が図れる。

### 実施例3

実施例3では、実施例1および実施例2で示した発明の例に基づき、実際に数値を示して例を説明する。ここでは電子透かし情報を1ビットとし、その埋め込み繰り返し回数 $n$ を127回とし、電子透かし情報の全埋め込み対象領域から任意の1ビット電子透かし系列を抽出したときにビット1が抽出される確率 $q$ を $1/2$ とする。信頼性のしきい値 $\alpha$ を0.99999（99.999%の意）とすると、図3における $x_0$ は36、 $x_1$ は90である。すなわち、以上の条件の下でこの発明は、電子透かし情報を、電子透かし系列（ $n$ ビット）に現れる1の個数が36以下である場合はビット0、90以上の場合はビット1、それ以外の場合は電子透かしが不明もしくは無しと判定する。電子透かし情報有りとは判定した場合、その正当率は99.999%以上を保証できる。

【0025】

以下は実験例を示す。

実験対象画像として $128 \times 128$ 画素の“lena”画像を用い、信頼度のしきい値 $\alpha$ を0.999999として実験を行なった。

### 実験1

1ビットの透かし情報“1”を秘密鍵情報“50, 000”を用いて127回繰り返し埋め込み、任意の秘密鍵情報を用いて透かし系列の読みとりを行なった。図7は、秘密鍵情報に対する読みとり透かし系列のビット1の個数を示したものである。縦軸は読みとった透かし系列におけるビット1の個数、横軸は秘密鍵情報の値を表している。ただし、透かし対象領域Aのビット1の出現頻度は $q = 0.492247$ であった。正しい秘密鍵（50, 000）を用いた場合、ビット1の個数が透かし有無の判定しきい値 $x_1$ より大きいことから、正当率99.9999%で透かし情報は1であると判定でき、正しくない秘密鍵を用いた場合はすべて透かし無しもしくは不明と判定した。

### 実験2



7 段の M 系列（初期状態 64）を用いて変調した透かし系列を埋め込み、任意の秘密鍵情報と初期状態が任意の M 系列を用いて実験 1 と同様の実験を行なった（図 8）。変調を行なうことにより、実験 1 のデータと比較して  $q$  の値は 0.500000 に、分散は 31.008265 から 31.718777 とほとんど変化しなかった。透かしが抽出できたのは、正しい秘密鍵情報と疑似乱数系列の組を用いたときのみであった。また、透かし対象領域 A の半分のデータに透かし系列を埋め込んだ場合、変調なしでは  $q = 0.741547$  であったのに対し、変調を行なうことで  $q = 0.499768$  という結果が得られた。

【0026】

【発明の効果】

1. 統計学における二項分布に基づき電子透かし情報を判定することに以下の効果がある。

－電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価でき、その値を電子透かしの信頼度のしきい値  $\alpha$  を用いて  $2(1 - \alpha)$  で抑えることができる。

【0027】

2. 電子透かし情報を埋め込む前に疑似乱数終りで変調することにより以下の効果がある。

－電子透かし情報の全埋め込み対象領域から任意の 1 ビット電子透かし系列を抽出したときにビット 1 が抽出される確率  $q$  の偏りを無くした。

－電子透かし抽出に必要な正しい電子透かしの秘密鍵情報と抽出した電子透かし系列を復調するのに必要な疑似乱数系列無しに  $q$  の偏りから電子透かしの有無ならびにその値を検知することが困難となった。

【0028】

－実装において、 $q = 1/2$  と仮定できるため、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、処理の高速化が図れる。

$\alpha$  は、抽出した情報の正当率の下限を示す指標であり、電子透かしシステムの内部で管理可能な情報となっている。これは、従来の電子透かしシステムに見ら

れた、抽出した電子透かし情報の正当率を利用者に提示するものより優れている点である。

【0029】

この発明は、誤り訂正符号と併用することでさらに大きな効果が得られる。すなわち、電子透かし情報の一部のビットだけが集中して壊れているような場合、抽出した情報は、一部のビットだけが不明で、それ以外のビット情報は正当性が高い状態にあると正確に判定できる。よって壊れたビット情報のみを誤り訂正することにより、確実に正しい情報が抽出できる。

【図面の簡単な説明】

【図1】

電子透かしシステムの概要を示す図。

【図2】

図1中の電子透かし抽出装置概要を示す図。

【図3】

電子透かし情報の判定を示す図。

【図4】

電子透かし情報再構成の概念を示す図。

【図5】

電子透かし抽出処理の手順を示す図。

【図6】

この発明の第2実施例の概要を示す図。

【図7】

透かし系列読みとり結果（変調なし）を示す図。

【図8】

透かし系列読みとり結果（変調あり）を示す図。

【書類名】 図面

【図 1】

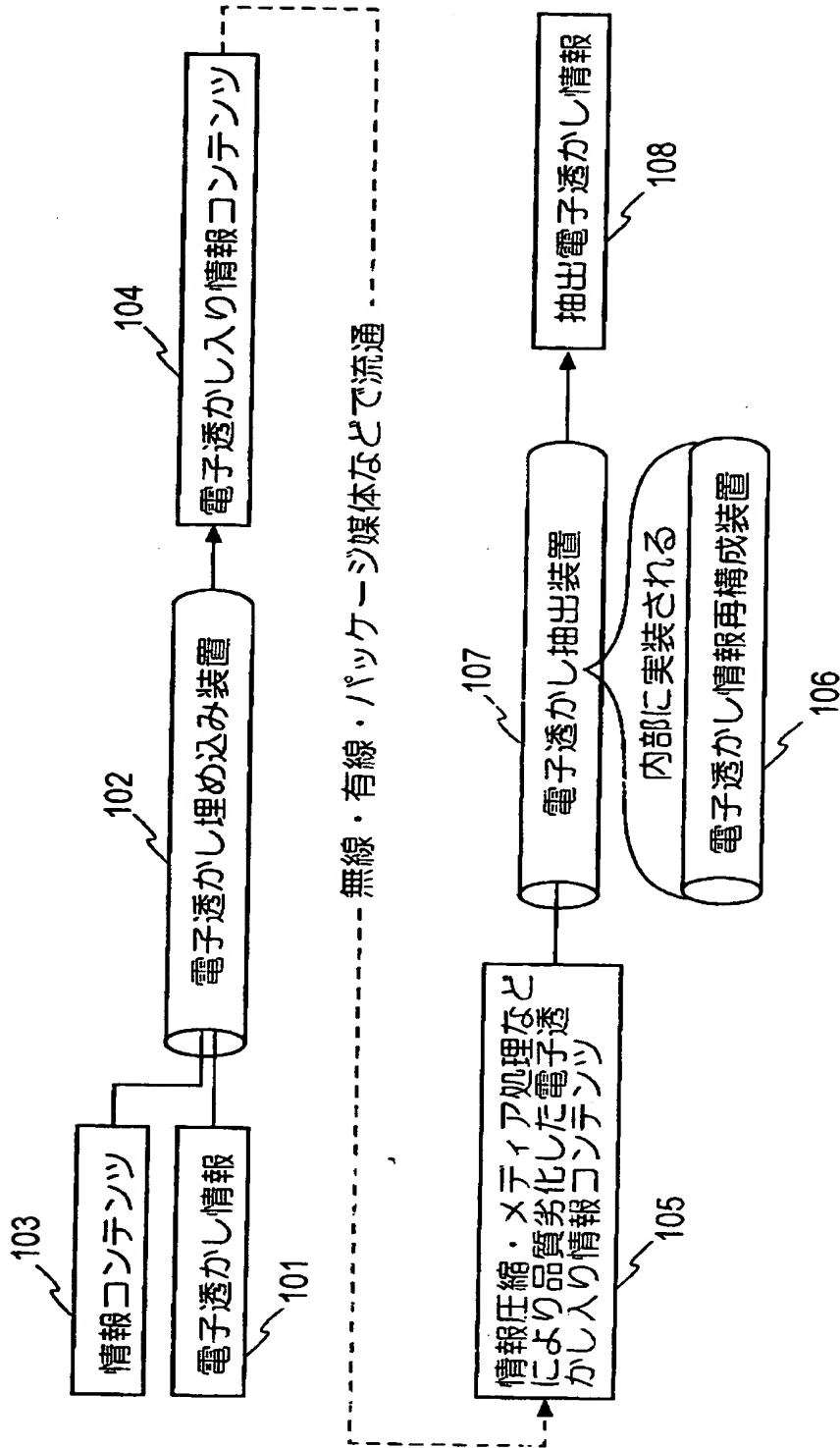


図 1

【図 2】

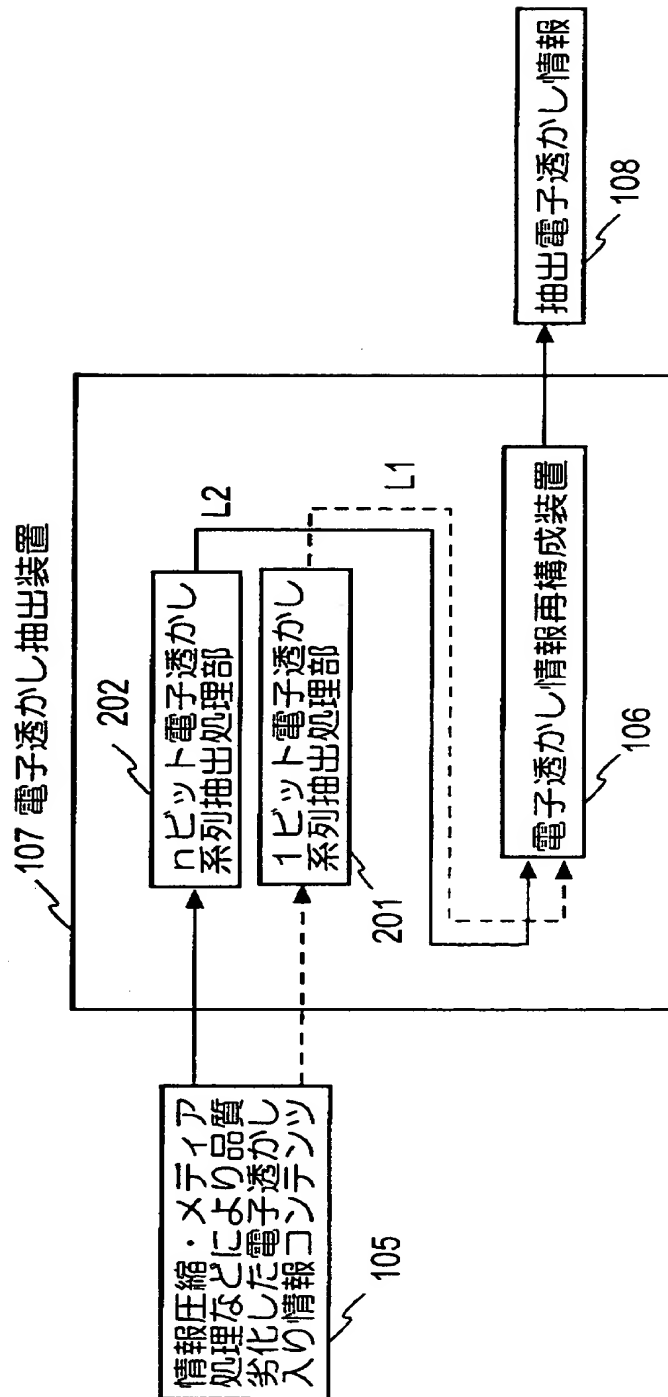


図 2

【図 3】

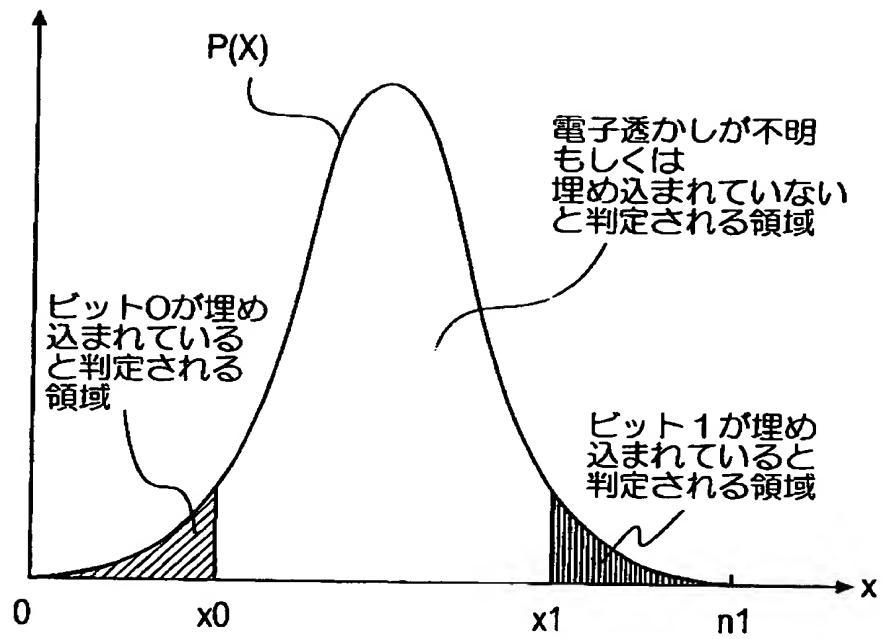


図 3

【図 4】

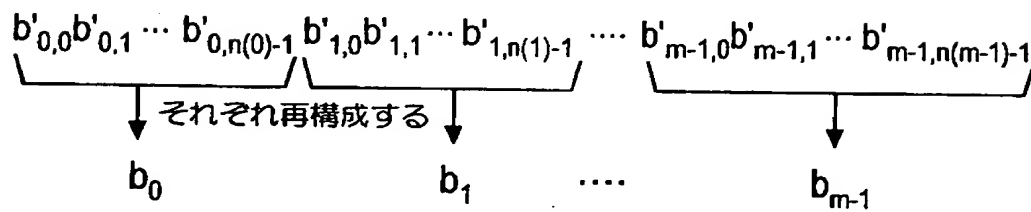
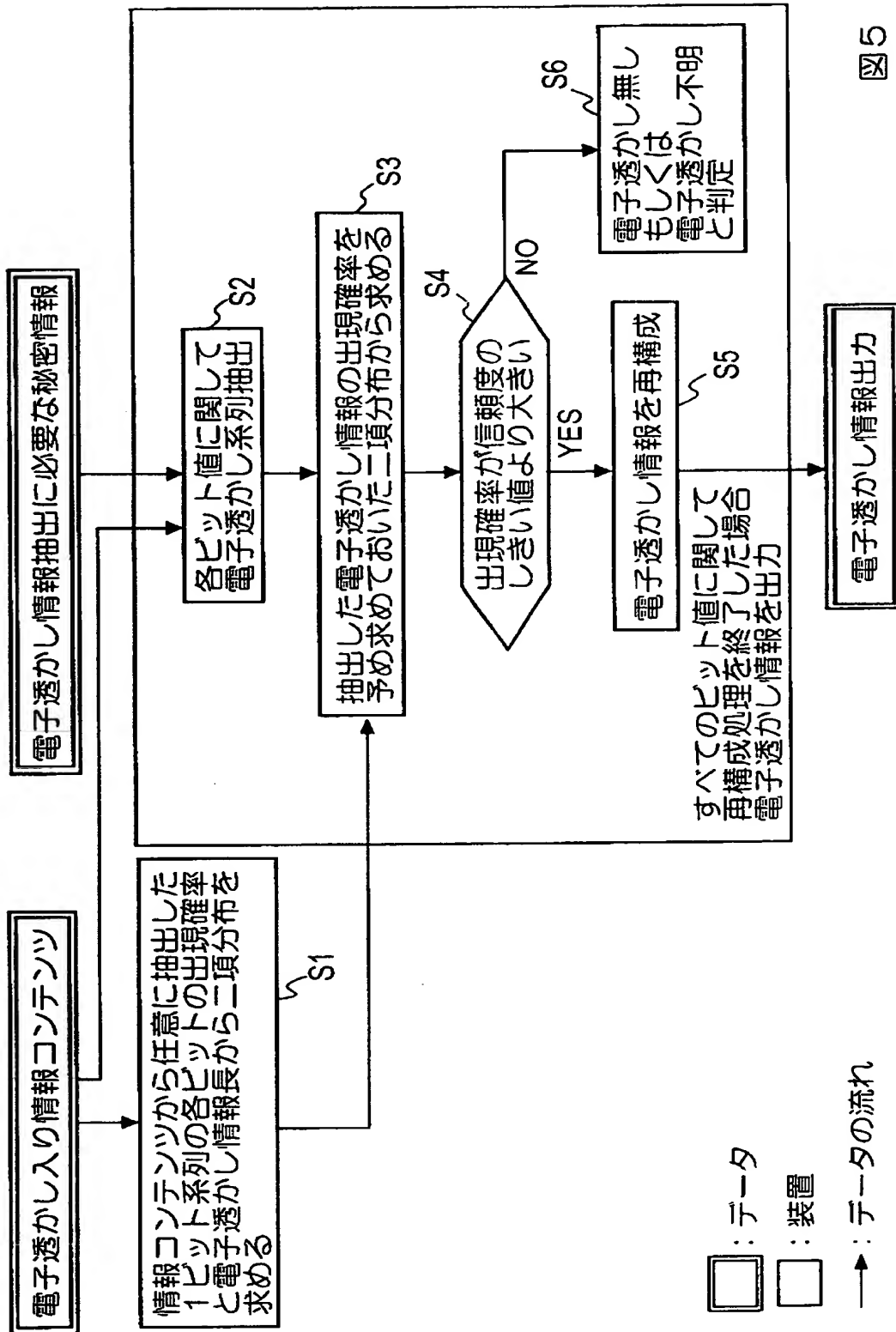


図 4

【図 5】



【図 6】

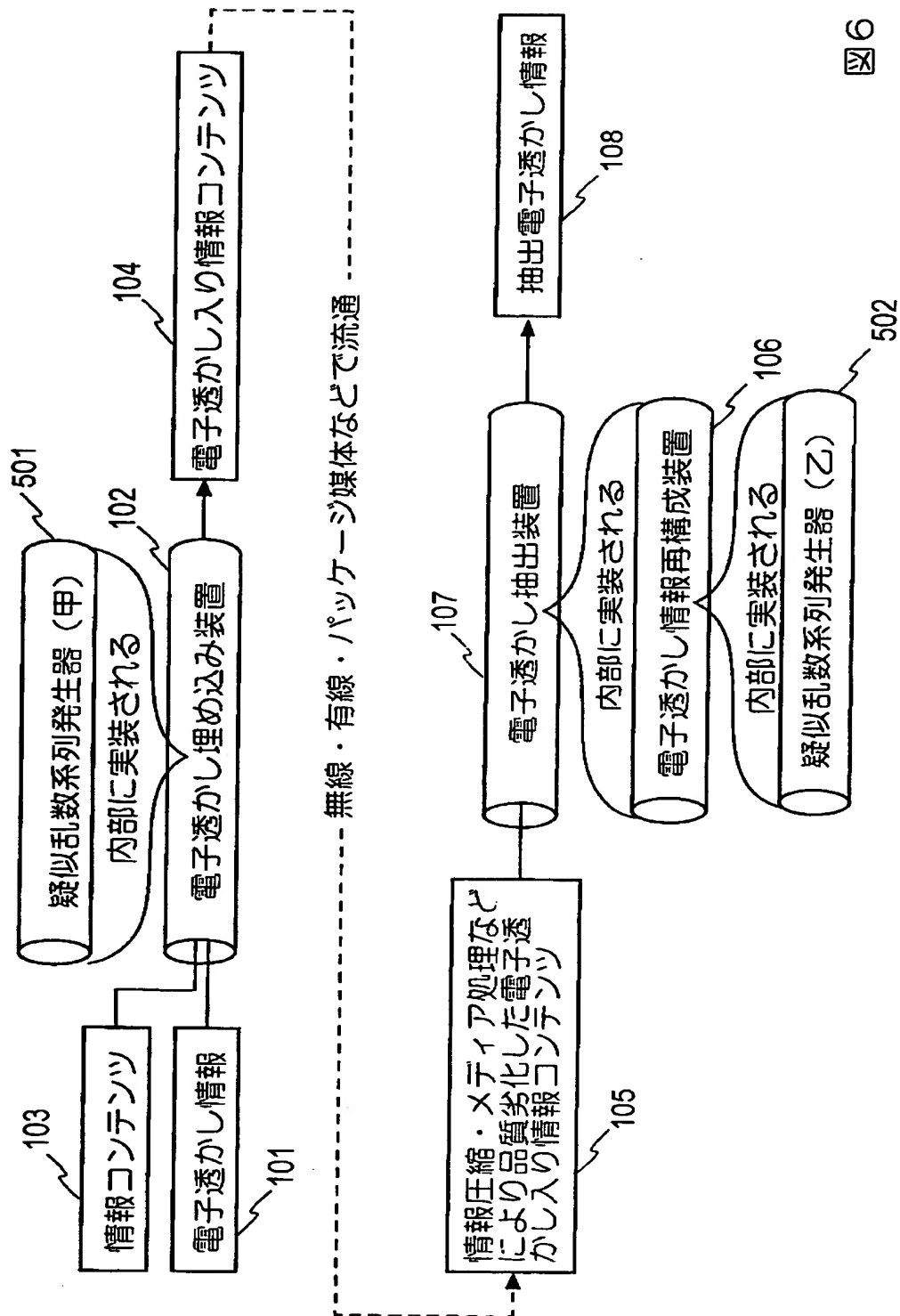


図 6

【図 7】

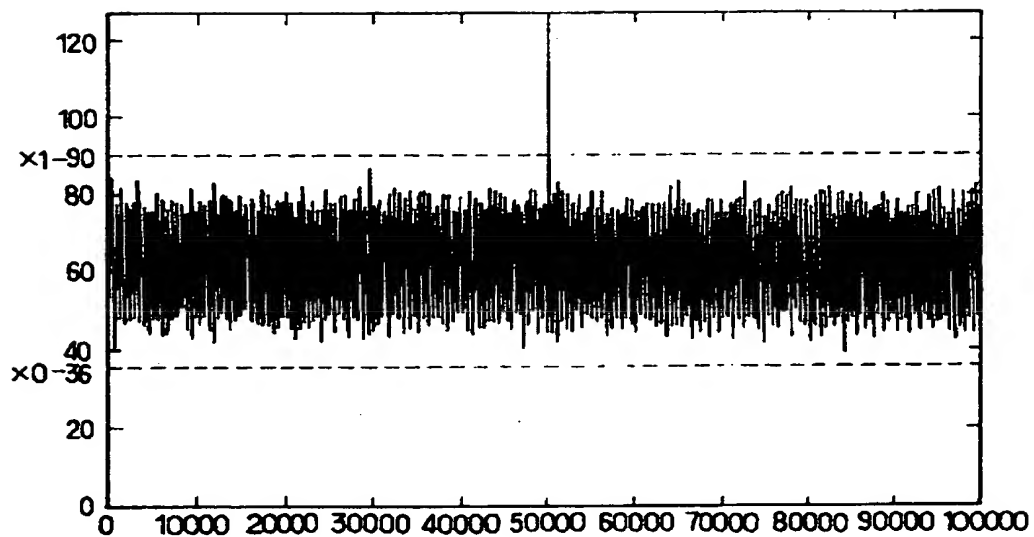


図 7

【図 8】

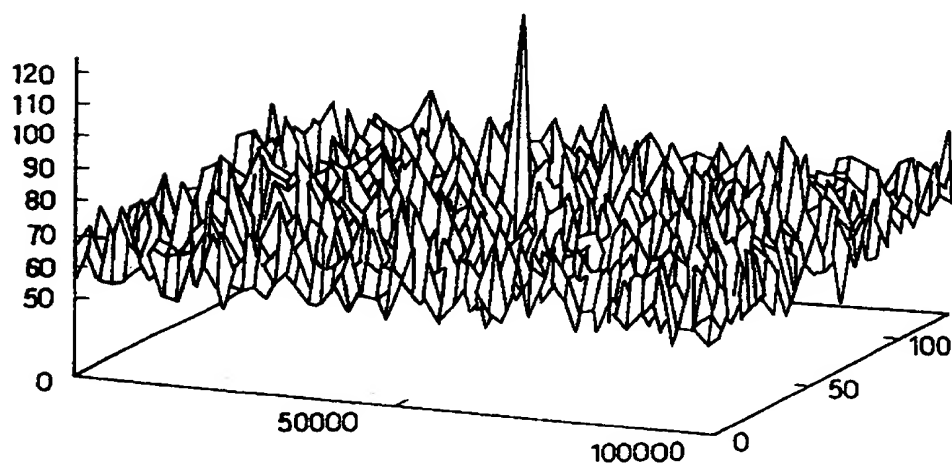


図 8



【書類名】 要約書

【要約】

【課題】 電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価する。

【解決手段】 情報コンテンツの透かし対象領域から無作為に1ビット透かし系列の抽出を行い、その時のビット0と1の出現確率  $1-q$  と  $q$  を求め、透かしが埋め込まれたのべ回数  $n_i$  ビットだけ透かし系列を抽出し、この時、 $n_i$  ビット列に1が  $k$  個現れる確率

$$P(x=k) = n_i C_k q^k \cdot (1-q)^{n_i-k}$$

その分布関数

$$F(x) = \sum_{k=0}^x n_i C_k q^k \cdot (1-q)^{n_i-k} \quad (0 \leq x \leq n_i)$$

より、透かし情報の信頼度のしきい値  $\alpha$  ( $1/2 < \alpha \leq 1$ ) に対し、 $0 \leq F(x=x_0) \leq 1-\alpha$  を満す最大の  $x_0$  と、 $\alpha \leq F(x=x_1) \leq 1$  を満す最小の  $x_1$  をそれぞれ透かし情報判定しきい値とする。

【選択図】 図3

【書類名】  
【訂正書類】

職権訂正データ  
特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】

000004226

【住所又は居所】

東京都新宿区西新宿三丁目19番2号

【氏名又は名称】

日本電信電話株式会社

【代理人】

申請人

【識別番号】

100066153

【住所又は居所】

東京都新宿区新宿四丁目2番21号 相模ビル

【氏名又は名称】

草野 卓

【選任した代理人】

【識別番号】

100100642

【住所又は居所】

東京都新宿区新宿4丁目2番21号 相模ビル 草

野特許事務所

【氏名又は名称】

稲垣 稔

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日 1995年 9月21日  
[変更理由] 住所変更  
住 所 東京都新宿区西新宿三丁目19番2号  
氏 名 日本電信電話株式会社
  
2. 変更年月日 1999年 7月15日  
[変更理由] 住所変更  
住 所 東京都千代田区大手町二丁目3番1号  
氏 名 日本電信電話株式会社